

DISTRIBUTION OF ELEMENTS OF COSETS OF SMALL SUBGROUPS AND APPLICATIONS

JEAN BOURGAIN, SERGEI KONYAGIN, AND IGOR SHPARLINSKI

ABSTRACT. We obtain a series of estimates on the number of small integers and small order Farey fractions which belong to a given coset of a subgroup of order t of the group of units of the residue ring modulo a prime p , in the case when t is small compared to p . We give two applications of these results: to the simultaneous distribution of two high degree monomials x^{k_1} and x^{k_2} modulo p and to a question of J. Holden and P. Moree on fixed points of the discrete logarithm.

1. INTRODUCTION

1.1. Estimates for the number of elements of small height in a coset of a small subgroup. We fix a prime number $p > 2$. By \mathbb{F}_p we denote the field of residues modulo p . For any element $x \in \mathbb{F}_p$ we define its integer height

$$|x| = \min\{|a| : a \in \mathbb{Z}, a \equiv x \pmod{p}\}$$

and its rational height

$$\|x\| = \min\{\max(|a|, b) : a \in \mathbb{Z}, b \in \mathbb{N}, a \equiv bx \pmod{p}\}.$$

Note that by pigeonhole principle,

$$|x| \leq p/2, \quad \|x\| \leq \sqrt{p}.$$

Moreover, if $\|x\| \leq \sqrt{p/2}$ then the numbers $a \in \mathbb{Z}$, $b \in \mathbb{N}$ with $|a| \leq \|x\|$, $b \leq \|x\|$, $a \equiv bx \pmod{p}$ are uniquely defined. Also, the rational height is defined for a rational number x as

$$\|x\| = \min\{\max(|a|, b) : a \in \mathbb{Z}, b \in \mathbb{N}, x = a/b\}.$$

As usual, we use $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ to denote the multiplicative group of \mathbb{F}_p .

Date: January 13, 2013.

2000 *Mathematics Subject Classification.* Primary 11A15; Secondary 11L07, 11N25.

Key words and phrases. congruence, multiplicative group of residues, smooth number, discrete logarithm.

If $t \mid p-1$ then there is a unique multiplicative subgroup $G \subseteq \mathbb{F}_p^*$. For $a \in \mathbb{F}_p$ we denote

$$aG = \{ag : g \in G\}.$$

Our aim is to estimate the cardinality of the sets

$$U(k, t, a) = \{x : x \in aG, |x| \leq k\},$$

$$V(k, t, a) = \{x : x \in aG, \|x\| \leq k\}.$$

These quantities are important for estimates of exponential sums in \mathbb{F}_p and for analysis of distribution of cosets of G in \mathbb{F}_p . Estimates for $\#U(k, t, a)$ and for $\#V(k, t, a)$ have been obtained in [17] and [5] where the case of “large” t and k , that is, for $\log k \asymp \log t \asymp \log p$ (where $A \asymp B$ means that $A = O(B)$ and $B = O(A)$) has been studied. In this paper our main interest is related to the case of small G ($\log t = o(\log p)$; in particular, $\log t \asymp \log \log p$). It is proved in [3] that in a very general situation with rather small t and rather large k we have $\#U(k, t, a) = o(t)$. For smaller k (say, $k \leq p^{0.1}$) the problem is easier. In this paper we prove some explicit estimates of $\#U(k, t, a)$ and for $\#V(k, t, a)$ for such k and small G and apply these results to the problem of simultaneous distribution of two powers in \mathbb{F}_p (see [1]). If both parameters t and k are very small we establish some upper bounds for $\#U(k, t, a)$ and for $\#V(k, t, a)$, usually much better than the trivial estimates

$$\#U(k, t, a) \leq \min\{2k, t\} \quad \text{and} \quad \#V(k, t, a) \leq \min\{2k^2, t\}.$$

These results are applied to estimation of fixed points of the discrete logarithms.

We also noted that in the case when k and t are of about the same size one can estimate $\#U(k, t, a)$ by using the results and techniques of [7], based on [4, Theorem 1.1] that gives an explicit version of the sum-product theorem and of [8] which is based on estimates of [9] on the number of divisors in a short interval of an integer n .

To formulate our results, we need some notation.

Let $x, y > 0$. A positive integer n is called y -smooth if it is composed of prime numbers up to y . The $\Psi(x, y)$ function is defined as the number of y -smooth positive integers that are up to x .

As usual, we use (a, b) to denote the greatest common divisor of integers a and b (with $a^2 + b^2 > 0$).

Finally, we also use p_k to denote the k th prime.

We fix a prime number $p > 2$. For any positive integer $1 < k < p/2$ we define the quantity

$$(1.1) \quad r_0(k) = \left\lfloor \frac{\log(p/2)}{\log k} \right\rfloor$$

Furthermore, let $t \in \mathbb{N}$ be another parameter, then we define

$$(1.2) \quad s_0(k, t) = \max \left\{ s : \binom{r_0(k) + s}{s} \leq t \right\}.$$

We observe that $r_0(k)$ decreases and $s_0(k, t)$ increases as k and t increase.

Theorem 1. *For any $a \in \mathbb{F}_p^*$ we have*

$$\#\{|x| : x \in U(k, t, a)\} \leq \Psi(k, p_{s+1})$$

where $s = s_0(k, t)$.

Theorem 2. *Let $a \in \mathbb{F}_p^*$ and $x_0 \in U(k, t, a)$*

$$\#\{|x| : x \in U(k, t, a), (x, x_0) = 1\} \leq \Psi(k, p_s)$$

where $s = s_0(k, t)$.

If the coset is G itself then we can take $x_0 = 1$. Thus, we have the following estimate for the number of small elements in a subgroup.

Corollary 3. *We have*

$$\#\{|x| : x \in U(k, t, 1)\} \leq \Psi(k, p_s)$$

where $s = s_0(k, t)$.

Remark 1. If we are interested in counting the number of x such that $x \in U(k, t, a)$ and $1 \leq x \leq k$ then sometimes it is possible to estimate this number slightly better than in Theorem 1 by replacing $r_0(k)$ in the definition of $s_0(k, t)$ with

$$\tilde{r}_0(k) = \left\lfloor \frac{\log p}{\log k} \right\rfloor.$$

A similar improvement can be made for Theorem 2 as well.

To study elements of small rational height in cosets of subgroups, we also define

$$r_1(k) = \lfloor r_0(k)/2 \rfloor = \left\lfloor \frac{\log(p/2)}{2 \log k} \right\rfloor.$$

If $r_1(k) \geq 1$ (that is, $k \leq (p/2)^{1/2}$) we also define

$$s_1(k, t) = \max \left\{ s : \binom{r_1(k) + s}{s} \leq t \right\}.$$

Next, we denote for $s \in \mathbb{N}$

$$\tilde{\Phi}(k, s) = \sum_{i=0}^s \binom{s}{i} \Psi(k, p_i) \Psi(k, p_{s-i}).$$

Also, we consider that $\tilde{\Phi}(k, 0) = 1$.

Theorem 4. *For any $a \in \mathbb{F}_p^*$ we have*

$$\#\{|x| : x \in V(k, t, a)\} \leq \tilde{\Phi}(k, s+1)$$

where $s = s_1(k, t)$.

Theorem 5. *We have*

$$\#\{|x| : x \in V(k, t, 1)\} \leq \tilde{\Phi}(k, s)$$

where $s = s_1(k, t)$.

Theorems 1–5 can be useful only for very small k . For example, if $k \gg p^\delta$ with a fixed $\delta > 0$ then the estimates given by these theorems are trivial. However, using ideas of their proofs we can estimate $\#V(k, t, a)$ non-trivially for very small subgroups G and not too small k . In particular, if $\delta \in (0, 1/10)$ is fixed and $k \asymp p^\delta$ then the following theorem is nontrivial for a certain range of t . Denote

$$r_2(k) = \left\lfloor \frac{\log(p/2)}{8 \log k} - \frac{1}{4} \right\rfloor.$$

Theorem 6. *Let $s \in \mathbb{N}$. For any $a \in \mathbb{F}_p^*$ we have*

$$\#V(k, t, a) \leq \max \left(2\tilde{\Phi}(k^2, s-1), \binom{r+s}{s}^{-1} t \right)$$

where $r = r_2(k)$.

We also have:

Theorem 7. *Let $s \in \mathbb{N}$. We have*

$$\#V(k, t, 1) \leq \max \left(2\tilde{\Phi}(k, s-1), \binom{r+s}{s}^{-1} t \right)$$

where $r = r_2(k)$.

We do not prove analogs of Theorem 6 and 7 for integer heights. However, notice that some estimates for $\#U(k, t, a)$ can be deduced using the trivial inequality $\#U(k, t, a) \leq \#V(k, t, a)$.

1.2. On solutions of systems of congruences. A general problem is to estimate, for given r, a_i, k_i, l_i ($i = 1, \dots, r$), the number of solutions of a system of congruences

$$(1.3) \quad a_i x^{k_i} \equiv l_i + y_i \pmod{p}$$

in the box

$$(1.4) \quad (x, y_1, \dots, y_r) \in \mathbb{F}_p^* \times \prod_{i=1}^r [1, N_i].$$

For integers $1 \leq k_1 < \dots < k_r < p-1$ which satisfy the conditions

$$(1.5) \quad (k_i, p-1) < p^{1-\varepsilon}, \quad 1 \leq i \leq r,$$

and

$$(1.6) \quad (k_i - k_j, p-1) < p^{1-\varepsilon}, \quad 1 \leq j < i \leq r,$$

J. Bourgain [2] has established the following result.

Lemma 8. *Given $r \in \mathbb{N}$ and $\varepsilon > 0$, there is $\delta > 0$ depending only on r and ε , such that for a sufficiently large prime p and $1 \leq k_1 < \dots < k_r < p-1$ satisfying (1.5) and (1.6), for $(a_1, \dots, a_r) \in \mathbb{F}_p^r \setminus \{\mathbf{0}\}$ the bound holds*

$$\max_{(a_1, \dots, a_r) \in \mathbb{F}_p^r \setminus \{\mathbf{0}\}} \left| \sum_{x \in \mathbb{F}_p} \exp \left(\frac{2\pi i}{p} (a_1 x^{k_1} + \dots + a_r x^{k_r}) \right) \right| < p^{1-\delta}.$$

Remark 2. The condition (1.6) is essential, as for instance the example $x - x^{(p+1)/2}$ shows.

Using standard arguments, one can deduce from Lemma 8 the following.

Corollary 9. *Given $r \in \mathbb{N}$ and $\varepsilon > 0$, there are $\delta > 0$ and C , depending only on r and ε , with the following property. If $p > C$ is a prime and $1 \leq k_1 < \dots < k_r < p-1$ satisfy (1.5) and (1.6) then for $(a_1, \dots, a_r) \in \mathbb{F}_p^r \setminus \{\mathbf{0}\}$, $l_1, \dots, l_r \in \mathbb{F}_p$, and $N_1, \dots, N_r \in \mathbb{N}$, $N_1, \dots, N_r \leq p$, the number N of solutions of the system of congruences (1.3) satisfies the inequalities*

$$|N - N_1 \dots N_r / p^{r-1}| < p^{1-\delta}.$$

In particular, we have nontrivial solutions if

$$N_1 \dots N_r > p^{r-\delta}.$$

In [1, Theorem 17] the existence of solutions is proved under weaker restrictions on differences $k_i - k_j$, namely

$$(k_i - k_j, p-1) < \frac{p}{B} \quad (1 \leq j < i \leq r)$$

instead of (1.6), where B depends only on r and ε , which however are not enough for getting an upper estimate on the number of solutions of the same order $N_1 \cdots N_r / p^{r-1}$.

Furthermore, the estimates for the number of solutions of two congruences are given in [1, Theorem 19] in a more precise form under the conditions

$$(1.7) \quad (k_i, p-1) < p^{1-\varepsilon} \quad (i = 1, 2) \quad \text{and} \quad (k_1 - k_2, p-1) < \frac{p-1}{2}.$$

More precisely, for

$$(1.8) \quad a_1, a_2 \in \mathbb{F}_p^*, \quad l_1, l_2 \in \mathbb{F}_p, \quad N_1, N_2 \in \mathbb{N},$$

we define

$$I = \left\{ x \in \mathbb{F}_p^* : \begin{array}{l} \exists (n_1, n_2) \in [1, N_1] \times [1, N_2], \\ a_j x^{k_j} \equiv l_j + n_j \pmod{p} \quad (j = 1, 2) \end{array} \right\}.$$

Then by [1, Theorem 19], for every $\varepsilon > 0$ there is $\eta > 0$, such that the following holds. If k_1, k_2 satisfy (1.7) then for $1 \leq N_1, N_2 \leq p$ and any $\delta \in (0, \eta)$ we have

$$(1.9) \quad \#I \geq \left(\frac{N_1 N_2}{p} - C p^{1-\delta} \right) \left(1 - \max \left(\frac{2(k_1 - k_2, p-1)}{p-1}, 5\delta \right) \right),$$

where $C > 0$ is an absolute constant.

Remark 3. The estimate is nontrivial if $\delta < 1/5$ and $N_1 N_2 > C p^{2-\delta}$.

Thus, the bound (1.9) gives a nontrivial estimate for the number of solutions under very weak assumptions on $k_1 - k_2$. If $(k_1 - k_2, p-1)$ is essentially smaller than p then we can get a better lower estimate.

Theorem 10. *There exists an absolute constant $C > 0$, and for every $\varepsilon > 0$ there is $\eta > 0$, such that the following holds. If $\Delta \in \mathbb{N}$, k_1, k_2, η , satisfy (1.7) as well as*

$$1 \leq N_1, N_2 \leq p, \quad \Delta \leq p^\eta,$$

then

$$(1.10) \quad \#I \geq \left(\frac{N_1 N_2}{p} - C p \Delta^{-1} \right) \left(1 - t^{-1} \max_{a \in \mathbb{F}_p^*} \#V(\Delta, t, a) \right),$$

where

$$t = \frac{p-1}{(k_1 - k_2, p-1)},$$

Using Theorem 10 and Theorem 6 one can estimate the number of solutions of a system of two congruences from below. We give some related examples.

1.3. Fixed points of the discrete logarithms. We consider some exponential congruences which are related to studying fixed points of the discrete logarithms in finite fields, see [6, 10, 14, 15, 16, 21]. For a prime p we denote by $F(p)$ the number of solutions of the congruence

$$(1.11) \quad g^h \equiv h \pmod{p}, \quad 1 \leq g, h \leq p-1,$$

with arbitrary integers g and h . J. Holden and P. Moree [16] have conjectured that

$$(1.12) \quad F(p) = (1 + o(1))p.$$

It has been shown in [5] that $F(p) = p + O(p^{4/5+\varepsilon})$ for a set of primes of relative density 1.

It is noted in [5, Bound (33)] that

$$F(p) \leq (p-1)\tau(p-1),$$

where $\tau(n)$ is the number of divisors of $n \in \mathbb{N}$. Therefore

$$(1.13) \quad F(p) \leq p \exp \left(\frac{(\log 2 + o(1)) \log p}{\log \log p} \right).$$

We note that in (1.13) and everywhere else in the paper, the argument of iterated logarithms is always assumed to be large enough so that the function is well-defined.

Towards the conjecture (1.12), here we prove the following upper estimate for $F(p)$.

Theorem 11. *We have*

$$F(p) = O(p).$$

We remark that though obtaining an asymptotic formula for $F(p)$ seems to be difficult, rather elementary arguments imply the lower bound

$$(1.14) \quad F(p) \geq p + O(p^{3/4+o(1)}).$$

It is likely that the arguments of [5] can be used to get a better remainder term in (1.14); we do not try to optimise it in this paper.

1.4. Notation. We recall that $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that the inequality $|U| \leq cV$ holds with some constant $c > 0$. Sometimes we write $U = O_\lambda(V)$, $U \ll_\lambda V$ and $V \gg_\lambda U$ to emphasise that the implied constant may depend on a certain parameter λ . We also write $U \asymp V$ if $U \ll V \ll U$.

2. DISTRIBUTION OF ELEMENTS OF COSETS OF SMALL SUBGROUPS

2.1. Proof of Theorem 1. Take a maximal possible set

$$\{x_0, x_1, \dots, x_\ell\} \subseteq \mathbb{Z}$$

of multiplicatively independent elements of $U(k, t, a)$. We claim that

$$(2.1) \quad \ell \leq s.$$

Indeed, let

$$Y = \{x_0^{u_0} x_1^{u_1} \dots x_\ell^{u_\ell} \in \mathbb{Z} : u_0, \dots, u_\ell \geq 0, u_0 + \dots + u_\ell = r\}$$

where $r = r_0(k)$.

For any $y \in Y$ the exponents u_0, \dots, u_ℓ are uniquely defined due to multiplicative independence of x_0, \dots, x_ℓ . Therefore,

$$(2.2) \quad \#Y = \binom{r + \ell}{\ell}.$$

Next, for any $y \in Y$ we have $|y| \leq k^r < p/2$. Thus, different elements of $y \in \mathbb{Z}$ are different as elements of \mathbb{F}_p as well. Finally, $Y \subseteq a^{\ell+1}G$. Hence, $\#Y \leq t$. Comparing this inequality with (2.2) and recalling the definition (1.2) of $s_0(k, t)$ we get (2.1).

Take the largest possible n so that $p_n \leq k$ and define the matrix

$$A = (\alpha_{i,j})_{0 \leq i \leq \ell}^{1 \leq j \leq n}$$

of exponents in the prime number factorizations

$$|x_i| = \prod_{j=1}^n p_j^{\alpha_{i,j}}, \quad 0 \leq i \leq \ell.$$

By the choice of x_0, \dots, x_s , the matrix A is of full rank $\ell + 1$ and for any element

$$x = \pm \prod_{j=1}^n p_j^{\alpha_j} \in U(k, t, a)$$

the vector $(\alpha_1, \dots, \alpha_n)$ is a linear combination of rows of the matrix A with rational coefficients. We take a non-singular $(\ell + 1) \times (\ell + 1)$ submatrix B of A . Let the columns of B correspond to prime numbers $q_1 < \dots < q_{\ell+1}$.

For any $x \in U(k, t, a)$ we define $\mathbf{b}(x) = (\beta_1, \dots, \beta_{\ell+1})$ by

$$q_j^{\beta_j} \mid x \quad \text{and} \quad q_j^{\beta_j+1} \nmid x, \quad 1 \leq j \leq \ell + 1.$$

We denote the rows of B by

$$\mathbf{b}_i = (\beta_{i,1}, \dots, \beta_{i,\ell+1}), \quad 0 \leq i \leq \ell.$$

So,

$$B = (\beta_{i,j})_{0 \leq i \leq \ell}^{1 \leq j \leq \ell+1}.$$

We see that $\mathbf{b}_i = \mathbf{b}(x_i)$.

We claim that different elements $|x|$ with $x \in U(k, t, a)$ define different vectors $\mathbf{b}(x)$. Indeed, the vector $\mathbf{b}(x)$ determines rational numbers u_0, \dots, u_ℓ so that

$$\mathbf{b}(x) = \sum_{i=0}^{\ell} u_i \mathbf{b}_i.$$

Then

$$|x| = \prod_{i=0}^{\ell} |x_i|^{u_i}$$

is also uniquely determined by $\mathbf{b}(x)$.

It suffices to estimate the number of possible vectors $\mathbf{b}(x)$ with $x \in U(k, t, a)$. We note that

$$\prod_{j=1}^{s+1} p_j^{\beta_j(x)} \leq \prod_{j=1}^{s+1} q_j^{\beta_j(x)} \leq |x| \leq k$$

We now see that different elements $|x|$ with $x \in U(k, t, a)$ define different $p_{\ell+1}$ -smooth numbers, thus

$$\#U(k, t, a) \leq \Psi(k, p_{\ell+1}).$$

Using (2.1) completes the proof.

2.2. Proof of Theorem 2. Now we take a maximal possible set

$$\{x_1, \dots, x_\ell\} \subseteq \mathbb{Z}$$

of multiplicatively independent elements of $U(k, t, a)$ with $(x_0, x_j) = 1$ for $j = 1, \dots, \ell$. The inequality (2.1) can be proved in a similar way. If $y = x_0^{u_0} x_1^{u_1} \dots x_s^{u_s}$ then the number $|x_0|^{u_0}$ is determined as the largest power of $|x_0|$ dividing y . The exponents u_1, \dots, u_ℓ are uniquely defined due to multiplicative independence of x_1, \dots, x_ℓ and the equality

$$x_1^{u_1} \dots x_\ell^{u_\ell} = \pm y x_0^{-u_0}.$$

The matrix

$$A = (\alpha_{i,j})_{1 \leq i \leq \ell}^{1 \leq j \leq n}$$

is defined by the equalities

$$|x_i| = \prod_j p_j^{\alpha_{i,j}}, \quad 1 \leq i \leq \ell.$$

The rest of the proof is the same as in Theorem 1.

2.3. Proof of Theorem 4. Similarly to the proof of Theorem 1 we take a maximal possible set

$$\{x_0, x_1, \dots, x_\ell\} \in \mathbb{Q}$$

of multiplicatively independent elements of $V(k, t, a)$. Now we have to verify that

$$(2.3) \quad \ell \leq s = s_1(k, t).$$

To do so, we define

$$Y = \{x_0^{u_0} x_1^{u_1} \dots x_\ell^{u_\ell} \in \mathbb{Q} : u_0, \dots, u_\ell \geq 0, u_0 + \dots + u_\ell = r\}$$

where $r = r_1(k)$. The proof of (2.3) follows the proof of (2.1). The distinction is that now for any $y \in Y$ we have $\|y\| \leq k^r < \sqrt{p/2}$, and thus different rational values of y with this condition get reduced to different elements of \mathbb{F}_p .

We also choose prime numbers $q_1 < \dots < q_{\ell+1}$ as in the proof of Theorem 1. Now we have to estimate the number of rational numbers of the form

$$m = \prod_{j=1}^{s+1} q_j^{\beta_j} \in \mathbb{Q} : \|m\| \leq k.$$

Denote

$$J_+ = \{j : \beta_j \geq 0\}, \quad m_+ = \prod_{j \in J_+} q_j^{\beta_j} \in \mathbb{N},$$

$$J_- = \{j : \beta_j < 0\}, \quad m_- = \prod_{j \in J_-} q_j^{-\beta_j} \in \mathbb{N}.$$

So, $m = m_+/m_-$, $m_+ \leq k$, $m_- \leq k$. For a fixed $i = \#J_+$ there are $\binom{\ell+1}{i}$ ways to select $J_+ \subseteq 1, \dots, \ell+1$. As J_+ and J_- have been chosen, there are at most $\Psi(k, p_i)$ possible values for m_+ and at most $\Psi(k, p_{\ell-i+1})$ possible values for m_- . Combining these estimates we complete the proof.

2.4. Proof of Theorem 5. We follow the proof of Theorem 4. Now we take a maximal possible set $\{x_1, \dots, x_s\}$ of multiplicatively independent elements of $V(k, t, 1)$ and define

$$Y = \{x_1^{u_1} \dots x_\ell^{u_\ell} \in \mathbb{Q} : u_1, \dots, u_\ell \geq 0, u_1 + \dots + u_\ell \leq r\}.$$

2.5. Proof of Theorems 6 and 7. We prove Theorems 6 and 7 simultaneously.

We take a maximal possible set $\{x_1, \dots, x_\ell\}$ of multiplicatively independent elements of $V(k, t, 1)$. We consider separately two cases.

Case of $\ell < s$. Assume that $V(k, t, a) \neq \emptyset$ and fix $y_0 \in V(k, t, a)$. Then for any $y \in V(k, t, a)$ we have $y = xy_0$ for some $x \in V(k^2, t, 1)$. By the arguments from the proof of Theorem 6 the number of elements x satisfying these conditions is at most $2\tilde{\Phi}(k^2, \ell) \leq 2\tilde{\Phi}(k^2, s-1)$ as desired for Theorem 6. If $a = 1$ we take $y_0 = 1$ and we have $x = y \in V(k, t, 1)$. This gives the bound $\#V(k, t, 1) \leq 2\tilde{\Phi}(k, s-1)$ as desired for Theorem 7.

Case of $\ell \geq s$. Take the largest possible n so that $p_n \leq k$. Define the matrix

$$A = (\alpha_{i,j})_{1 \leq i \leq \ell}^{1 \leq j \leq n}$$

by equalities

$$|x_i| = \prod_{j=1}^n p_j^{\alpha_{i,j}}, \quad 1 \leq i \leq \ell.$$

By the choice of x_1, \dots, x_s , the matrix A has rank ℓ and for any element

$$x = \pm \prod_{j=1}^n p_j^{\alpha_j} \in V(k, t, 1)$$

the vector $\mathbf{a}(x) = (\alpha_1, \dots, \alpha_n)$ is a rational linear combination of rows of the matrix A . Equivalently, the vector $(\alpha_1, \dots, \alpha_n)$ belongs to the linear subspace Y over \mathbb{Q} generated by $\mathbf{a}(x_j)$, $j = 1, \dots, \ell$. We now assume that the elements x_1, \dots, x_n are chosen so that the parallelepiped $\mathcal{P}(x_1, \dots, x_\ell)$ with edges $\mathbf{a}(x_j)$, $j = 1, \dots, \ell$ has a maximal volume.

We claim that for any integer vector $(u_1, \dots, u_\ell) \neq 0$ we have

$$(2.4) \quad \|x\| > k^{1/2}, \quad x = \prod_{j=1}^{\ell} x_j^{u_j} \in \mathbb{Q}.$$

Indeed, assume that (2.4) does not hold. Without loss of generality, we can assume that $|u_1| \neq 0$. We consider a new system of multiplicatively independent elements of $V(k, t, 1)$ obtained by replacing a number x_1 in the system (x_1, \dots, x_ℓ) by x^2 . Then the volume of $\mathcal{P}(x^2, x_2, \dots, x_\ell)$ is the volume of $\mathcal{P}(x_1, \dots, x_\ell)$ multiplied by $2|u_1| > 1$. This does not agree with the choice of (x_1, \dots, x_ℓ) . So, (2.4) holds.

Now we consider the set

$$Y = \left\{ \prod_{j=1}^{\ell} x_j^{4u_j} y : u_0, \dots, u_\ell \geq 0, \right. \\ \left. u_0 + \dots + u_\ell \leq r, y \in V(k, t, 1) \right\} \subseteq \mathbb{Q},$$

where $r = r_2(k)$. Using (2.4) and the inequality $\|y_1/y_2\| \leq k^2$ for $y_1, y_2 \in V(k, t, 1)$, we deduce that different vectors (u_1, \dots, u_ℓ, y) define different elements of y . Therefore,

$$(2.5) \quad \#Y = \binom{r_2 + \ell}{\ell} \#V(k, t, 1).$$

Next, for any $y \in Y$ we have $\|y\| \leq k^{4r_0+1} < \sqrt{p/2}$. Thus, different rational values of y with this condition get reduced to different elements of \mathbb{F}_p . Finally, $Y \subseteq aG$. Hence, $\#Y \leq t$. Comparing this inequality with (2.5) we get

$$t \geq \binom{r_2 + \ell}{\ell} \#V(k, t, 1) \geq \binom{r_2 + s}{s} \#V(k, t, 1).$$

This completes the proof.

3. ESTIMATES FOR SETS OF SMOOTH NUMBERS

We need several estimates for $\Psi(x, y)$.

If y is small, we use the following result, see [13, Theorem 1.4]:

Lemma 12. *Uniformly for $x \geq y \geq 2$, we have*

$$\log \Psi(x, y) = Z \left(1 + O \left(\frac{1}{\log y} + \frac{1}{\log \log x} \right) \right),$$

where

$$Z = \frac{\log x}{\log y} \log \left(1 + \frac{y}{\log x} \right) + \frac{y}{\log y} \log \left(1 + \frac{\log x}{y} \right).$$

In particular, we have, see [13, Equation (1.14)]:

Corollary 13. *For any $\alpha > 1$ we have*

$$\Psi(x, (\log x)^\alpha) = x^{1-1/\alpha+o(1)} \quad (x \rightarrow \infty).$$

Moreover, for very small y the asymptotic formula for $\Psi(x, y)$ is known, see [13, Theorem 1.5]:

Lemma 14. *Uniformly for $2 \leq y \leq (\log x)^{1/2}$, we have*

$$\Psi(x, y) = \frac{1}{\pi(y)!} \prod_{p_j \leq y} \frac{\log x}{\log p_j} \left(1 + O \left(\frac{y^2}{(\log x) \log y} \right) \right).$$

Therefore:

Corollary 15. *For any $s \in \mathbb{N}$ and $x \geq \exp(p_s^2)$ we have*

$$\Psi(x, p_s) \ll (\log x)^s.$$

For large y we know the following estimate for $\Psi(x, y)$, see [13, Corollary 1.3]:

Lemma 16. *Let $x \geq y \geq 2$ and $u = (\log x)/\log y$. For any fixed $\varepsilon > 0$ we have*

$$\Psi(x, y) = xu^{-(1+o(1))u},$$

as y and u tend to infinity, uniformly in the range $y \geq (\log x)^{1+\varepsilon}$.

Moreover, in a smaller range an asymptotic formula for $\Psi(x, y)$ is known, see [13, Theorem 1.1 and Corollary 2.3].

Lemma 17. *Let $x \geq y \geq 2$ and $u = (\log x)/\log y$. For any fixed $\varepsilon > 0$ we have*

$$\Psi(x, y) = x\rho(u) \left(1 + O \left(\frac{\log(1+u)}{\log y} \right) \right),$$

uniformly in the range

$$y \geq \exp((\log \log x)^{(5/3)+\varepsilon}),$$

where

$$\rho(u) = \exp(-u(\log u + \log \log(u+2)) + O(1)).$$

is the Dickman function.

4. ON SOLUTIONS OF SYSTEMS OF CONGRUENCES

4.1. Discrepancy and exponential sums. We recall the notion of *discrepancy* which for a sequence of H points

$$(4.1) \quad \Gamma = (\gamma_{1,x}, \dots, \gamma_{m,x})_{x=1}^H$$

in the m -dimensional unit cube, is defined as

$$\Delta_\Gamma = \sup_{B \subseteq [0,1]^m} \left| \frac{T_\Gamma(B)}{H} - |B| \right|,$$

where $T_\Gamma(B)$ is the number of points of the sequence Γ in the box

$$B = [\alpha_1, \beta_1) \times \dots \times [\alpha_m, \beta_m) \subseteq [0, 1]^m$$

of volume $|B|$ and the supremum is taken over all such boxes.

A link between the discrepancy and exponential sums has been established independently by Koksma [18] and Szűsz [20], see also [11, Theorem 1.21].

Lemma 18. *For any integer $L > 1$ and sequence Γ of H points (4.1) the following bound holds*

$$\Delta_\Gamma \ll_m \frac{1}{L} + \frac{1}{H} \sum_{\substack{\lambda_1, \dots, \lambda_m \in \mathbb{Z} \\ 0 < |\lambda_1| + \dots + |\lambda_m| \leq L}} \prod_{j=1}^m \frac{1}{|\lambda_j| + 1} \left| \sum_{x=1}^H \exp \left(2\pi i \sum_{j=1}^m \lambda_j \gamma_{j,x} \right) \right|.$$

4.2. **The proof of Theorem 10.** Let

$$d = (k_1 - k_2, p - 1) \quad \text{and} \quad t = (p - 1)/d.$$

If $(k_1 - k_2, p - 1) < p^{1-\varepsilon/2}$ then the result follows from Corollary 9. So we assume that

$$d \geq p^{1-\varepsilon/2}.$$

Write $x = y^t z$. For any $z \in \mathbb{F}_p^*$ we denote

$$I_z = \{y \in \mathbb{F}_p^* : y^t z \in I\}.$$

Then

$$(4.2) \quad \#I = \frac{1}{p-1} \sum_{z \in \mathbb{F}_p^*} \#I_z.$$

Fix z . Since $y^{k_1 t} \equiv y^{k_2 t} \pmod{p}$, the condition $x \in I$ can be written as

$$(4.3) \quad a_j y^{k_1 t} z^{k_j} \equiv l_j + n_j \pmod{p}, \quad n_j \in [1, N_j], \quad j = 1, 2.$$

Now we denote

$$\mathcal{Z} = \{z \in \mathbb{F}_p^* : \|a_2 z^{k_2 - k_1} / a_1\| > \Delta\}.$$

To get a lower estimate for $\#I$ we take a sum over only $z \in \mathcal{Z}$.

First we estimate $\#\mathcal{Z}$. The multiset $\{z^{k_1 - k_2}\}$ is the subgroup G of \mathbb{F}_p^* of order t , and each element of G has multiplicity d . Therefore,

$$(4.4) \quad \#\mathcal{Z} = (1 - t^{-1} |V(\Delta, t, a_2/a_1)|) (p - 1).$$

Next, we estimate $\#I_z$ for $z \in \mathcal{Z}$. We note that the condition $z \in \mathcal{Z}$ implies that

$$\lambda_1 a_1 + \lambda_2 a_2 z^{k_2 - k_1} \not\equiv 0 \pmod{p}$$

for $0 < \max(|\lambda_1|, |\lambda_2|) \leq \Delta$. By Lemma 8 we have

$$\left| \sum_{y \in \mathbb{F}_p^*} \exp \left(\frac{2\pi i}{p} (y^{k_1 t} z^{k_1} (\lambda_1 a_1 + \lambda_2 a_2 z^{k_2 - k_1})) \right) \right| \leq p^{1-\delta}$$

for some $\delta > 0$ that depends only on ε . Thus by Lemma 18, applied with $m = 2$ and $L = \Delta$, we obtain

$$\#I_z = \frac{N_1 N_2}{p} + O(p/\Delta + p^{1-\delta} (\log \Delta)^2).$$

We observe that for $\eta \leq \delta/2$ and $\Delta \leq p^\eta$ we have

$$p^{1-\delta} (\log \Delta)^2 \ll p/\Delta.$$

Recalling (4.2) and the bound (4.4) we complete the proof.

4.3. Applications of Theorem 10: some examples. We consider the cases when N_1, N_2 are comparable to p . In our examples we use notation from the statement of Theorem 10 .

Corollary 19. *For any $A_1 > 0, A_2 > 0$ there exists some B such that if*

$$N_1 \geq A_1 p, \quad N_2 \geq A_1 p, \quad t \leq \frac{A_2 \log p}{\log \log p}$$

then

$$\#I \geq \frac{N_1 N_2}{p} \left(1 - \frac{B}{t}\right).$$

Indeed, we assume that p is large enough. We take $\Delta = [(\log p)^2]$. To estimate $\#V(\Delta, t, a)$ we apply Theorem 6 with $s = 1$.

Corollary 20. *For any $l \in \mathbb{N}, A_1 > 0, A_2 > 0$ there exists some B such that if*

$$N_1 \geq A_1 p, \quad N_2 \geq A_1 p, \quad t \geq \frac{A_2 (\log p)^l}{\log \log p}$$

then

$$\#I \geq \frac{N_1 N_2}{p} \left(1 - \frac{B (\log \log p)^l}{(\log p)^l}\right).$$

Indeed, we assume that p is large enough. We take $\Delta = [(\log p)^{l+1}]$. To estimate $\#V(\Delta, t, a)$ we apply Theorem 6 with $s = l$ observing that, due to Corollary 15, we have $\tilde{\Phi}(x, s-1) \ll_s (\log x)^{s-1}$ for $x \geq 2$.

If t is large one can use the following estimate.

Corollary 21. *For any $\eta \in (0, 1/2], \varepsilon > 0, A_1 > 0, A_2 > 0$ there exists some B such that if $t \leq p^\eta$ and*

$$N_1 \geq A_1 p, \quad N_2 \geq A_1 p$$

then

$$\#I \geq \frac{N_1 N_2}{p} \left(1 - B \frac{\log p + t^{(1+\varepsilon)/l}}{t}\right)$$

where $l = \lfloor 1/(2\eta) \rfloor$.

Proof. Again, we assume that p is large enough. We take $\Delta = \lfloor t/2 \rfloor$ and denote

$$\mathcal{A} = \{(u/v) : u \in \mathbb{Z}, v \in \mathbb{N}, |u| \leq \Delta, v \leq \Delta, \\ \exists x \in aG \text{ } vx \equiv u \pmod{p}\}.$$

By the definition of $V(\Delta, t, a)$, we can associate with any element $x \in V(\Delta, t, a)$ a rational number $u/v \in \mathcal{A}$ such that $vx \equiv u \pmod{p}$. Thus,

$$(4.5) \quad \#\mathcal{A} \leq \#V(\Delta, t, a).$$

Actually, the equality in (4.5) holds since $\Delta \leq \sqrt{p/2}$.

Now consider the set

$$\mathcal{A}^{(l)} = \{a_1 \dots a_l : a_1, \dots, a_l \in \mathcal{A}\}.$$

By [5, Corollary 3] we have

$$(4.6) \quad \#\mathcal{A}^{(l)} \gg \#\mathcal{A}^{l-\varepsilon}$$

where the implied constant in \gg depends on l and ε . On the other hand, any element of $\mathcal{A}^{(l)}$ has the form u/v , $u \in \mathbb{Z}$, $v \in \mathbb{N}$, $|u| \leq \Delta^l$, $v \leq \Delta^l$. Since $\Delta^l \leq \sqrt{p/2}$, distinct elements of $\mathcal{A}^{(l)}$ are distinct as elements of \mathbb{F}_p as well. Considering $\mathcal{A}^{(l)}$ as a subset of \mathbb{F}_p we see that $\mathcal{A}^{(l)} \subseteq a^l G$. Therefore,

$$(4.7) \quad \#\mathcal{A}^{(l)} \leq t.$$

Inequalities (4.5), (4.6) and (4.7) imply

$$\#V(\Delta, t, a) \ll t^{(1+\varepsilon)/l}.$$

The corollary follows from this estimate and Theorem 10. \square

5. FIXED POINTS OF THE DISCRETE LOGARITHMS

5.1. Preparations. For any divisor d of $p-1$ and $k = (p-1)/d$ we define the sets

$$X^*(k, p) = \{x : 1 \leq x \leq k, (x, k) = 1, x^k \equiv (-k)^k \pmod{p}\},$$

$$X(k, p) = \{x : 1 \leq x \leq k, x^k \equiv (-k)^k \pmod{p}\},$$

Let

$$T(d, p) = \#X^*(k, p).$$

It is known that

$$(5.1) \quad F(p) = \sum_{d|p-1} dT(d, p),$$

see [16, Equation (5)].

Lemma 22. *We have*

$$\sum_{h|k} T((p-1)/h, p) \leq \#X(k, p).$$

Proof. For $h \mid k$ we define the set

$$X(k, h, p) = \frac{k}{h} X^*(h, p).$$

Clearly,

$$(5.2) \quad \#X(k, h, p) = \#X^*(h, p) = T((p-1)/h, p).$$

For $x \in X^*(h, p)$ we have

$$\left(\frac{kx}{h}\right)^k = \left(\frac{k}{h}\right)^k (x^h)^{k/h} \equiv \left(\frac{k}{h}\right)^k ((-h)^h)^{k/h} = (-k)^k \pmod{p}.$$

Therefore, the sets $X(k, h, p)$ are subsets of $X(k, p)$. Moreover, these sets are disjoint since for $x \in X(k, h, p)$ we have $(x, k) = h/k$. Applying (5.2) we complete the proof. \square

We use the following estimate for $T(d, p)$, see [5, Bound (39)] with $\nu = 3$.

Lemma 23. *We have*

$$T(d, p) \leq (d^{-4/3}p + (p/d)^{1/3}) (p/d)^{o(1)}.$$

Following [5] we denote

$$D = p \exp\left(-4 \frac{\log p}{\log \log p}\right)$$

(we always assume that p is large enough). Then we have

$$(5.3) \quad \sum_{\substack{d \mid p-1, \\ d \leq D}} dT(d, p) = p + o(p),$$

as $p \rightarrow \infty$, see [5, Section 5]. It is convenient for us to take a sum over k . The identity (5.1) can be rewritten as

$$(5.4) \quad F(p) = (p-1) \sum_{k \mid p-1} \frac{T((p-1)/k, p)}{k}.$$

We now define the sums

$$S_p(K, L) = \sum_{\substack{k \mid p-1, \\ K \geq k > L}} \frac{T((p-1)/k, p)}{k}.$$

and denote

$$\begin{aligned} K_1 &= \exp \left(4 \frac{\log p}{\log \log p} \right), \\ K_2 &= \exp \left((\log p)^{0.4} \right), \\ K_3 &= \exp \left((\log \log p)^7 \right) \end{aligned}$$

So we see from (5.4) that

$$(5.5) \quad F(p) = (p-1)(S_p(p-1, K_1) + S_p(K_1, K_2) + S_p(K_2, K_3) + S_p(K_3, 0)).$$

Inequality (5.3) immediately implies

$$(5.6) \quad S_p(p-1, K_1) = 1 + o(1),$$

as $p \rightarrow \infty$. So, to prove Theorem 11 we have to estimate the sums $S_p(K_1, K_2)$, $S_p(K_2, K_3)$ and $S_p(K_3, 0)$.

Our main tools are Theorem 2 and estimates for sets of smooth numbers. Besides, for the sum $S_p(K_3, 0)$ we use some arguments which stem from functional analysis.

5.2. Preliminary estimates. We recall the definitions (1.1) and (1.2) of the functions $r_0(k)$ and $s_0(k, t)$. By Lemma 22, Theorem 2 in this case can be rewritten as follows:

Corollary 24. *We have*

$$\sum_{h|k} T((p-1)/h, p) \leq \#X(k, p) \leq \Psi(k, p_s)$$

where $s = s_0(k, k)$.

By the prime number theorem we have

$$(5.7) \quad \frac{p_j}{\log p_j} = j + O \left(\frac{j}{\log j} \right).$$

It is easy to estimate the number of small divisors of a positive integer in terms of the $\Psi(x, y)$ function. Moreover, we need to estimate the number of products of a small divisor of a fixed number by a small smooth number. For $m \in \mathbb{N}$, $m \geq 2$, $y > 0$, and $z > 0$ by $\tau(m, y, z)$ we denote the number of numbers $dl \leq z$ where d is a divisor of m and l is an y -smooth number. Several estimates on $\tau(m, 1, z)$ have recently been given in [12]. In particular our next estimate for $y = 1$ is essentially [12, Bound (7)].

Lemma 25. *We have $\tau(m, y, z) \leq \Psi(z, q)$ where q is the largest prime number with*

$$\prod_{\substack{y < \ell \leq q \\ \ell \text{ prime}}} \ell \leq m.$$

Proof. Let D be the set of divisors d of m such that all prime divisors of d are greater than y . Thus, we have to estimate the number of numbers $dl \leq z$ where $d \in D$ and l is an y -smooth number. Let $q_1 < q_2 < \dots < q_J$ be the prime divisors of m that are greater than y , and let $\tilde{p}_1 < \tilde{p}_2 < \dots$ be the primes greater than y . We associate with any number dl where l is y -smooth, $d \in D$ and

$$d = \prod_{j=1}^J q_j^{\alpha_j}$$

the number

$$l \prod_{j=1}^J \tilde{p}_j^{\alpha_j} \leq dl,$$

which is clearly q -smooth. Since this map is injection, the result now follows. \square

Corollary 26. *We have $\tau(m, 1, z) \leq \Psi(z, q)$ where q is the largest prime number with*

$$\prod_{\substack{\ell \leq q \\ \ell \text{ prime}}} \ell \leq m.$$

5.3. Some tools from functional analysis. Finally, we also need the following statement which is essentially based on linear algebra. Let \mathcal{X} be a linear space of real sequences $\mathbf{x} = (x_q)_{q \in \mathcal{P}}$, finitely supported on the set of primes \mathcal{P} .

Define

$$\mathcal{H}(\mathbf{x}) = \sum_{q \in \mathcal{P}} |x_q| \log q.$$

Also for a set $\mathcal{Q} \subseteq \mathcal{P}$ we use $\pi_{\mathcal{Q}}$ to denote the coordinate restriction on the sequences of \mathcal{X} , that is for $\mathbf{x} = (x_q)_{q \in \mathcal{P}} \in \mathcal{X}$ we have

$$\pi_{\mathcal{Q}}(\mathbf{x}) = (x_q)_{q \in \mathcal{Q}}.$$

We have the following:

Lemma 27. *Let $\mathcal{F} \subseteq \mathcal{X}$ be a finite whose elements have integer coordinates. Let a positive integers s, L, M be such that $L \geq M$;*

- (i) *all elements of \mathcal{F} generate a linear subspace $\langle \mathcal{F} \rangle$ of \mathcal{X} of dimension $\dim \langle \mathcal{F} \rangle \leq s$;*

- (ii) $\mathcal{H}(\mathbf{x}) < L$ for $\mathbf{x} \in \mathcal{F}$;
- (iii) for any subset $\mathcal{Q} \subseteq \mathcal{P}$ with

$$(5.8) \quad \sum_{q \in \mathcal{Q}} \log q < M$$

the sequences $\pi_{\mathcal{P} \setminus \mathcal{Q}}$ is one-to-one on \mathcal{F} .

Then

$$\#\mathcal{F} < (cL/M)^s$$

for some absolute constant c .

Proof. We take a sufficiently large prime q_0 and let \mathcal{X}_0 be (a finitely dimensional) space of all real sequences $\mathbf{x} = (x_q)_{q \in \mathcal{P}_0}$ where $\mathcal{P}_0 = \{q \in \mathcal{P}, q \leq q_0\}$. We require that q_0 is so large that all elements of \mathcal{F} are supported on \mathcal{P}_0 . Thus, we can consider \mathcal{F} as a subset of \mathcal{X}_0 . Reduction the lemma to a finite dimensional subspace is caused by the using of the Hahn-Banach separation theorem which has a simpler form in the finite dimensional case.

Denote

$$\mathfrak{B} = \{\mathcal{B} \subseteq \mathcal{P}_0 : \#\mathcal{B} \leq s, \pi_{\mathcal{B}} \text{ is one-to-one on } \mathcal{F}\}$$

We see from the condition (i) that $\mathfrak{B} \neq \emptyset$. Moreover if $\mathcal{Q} \subseteq \mathcal{P}$ satisfies (5.8) then there exists $\mathcal{B} \in \mathfrak{B}$ with $\mathcal{B} \cap \mathcal{Q} = \emptyset$. Indeed, by (iii), $\pi_{\mathcal{P} \setminus \mathcal{Q}}$ is one-to-one map from \mathcal{F} to $\mathcal{G} = \pi_{\mathcal{P} \setminus \mathcal{Q}}(\mathcal{F})$. Since by (i) the linear subspace $\langle \mathcal{G} \rangle = \pi_{\mathcal{P} \setminus \mathcal{Q}}(\langle \mathcal{F} \rangle)$ of \mathcal{X}_0 is of dimension at most s , there is $\mathcal{B} \subseteq \mathcal{P} \setminus \mathcal{Q}$ with $\#\mathcal{B} \leq s$ and such that $\pi_{\mathcal{B}}$ is one-to-one on $\langle \mathcal{G} \rangle$. Hence $\pi_{\mathcal{B}}$ is one-to-one on \mathcal{G} and \mathcal{F} .

Let $\text{conv } \mathfrak{B}$ be the convex hull in \mathcal{X}_0 of characteristic functions of all possible sets treated as elements of $\mathcal{B} \in \mathfrak{B}$.

We claim that there exists an element $\beta = (\beta_q)_{q \in \mathcal{P}} \in \text{conv } \mathfrak{B}$ such that

$$(5.9) \quad 0 \leq \beta_q < 2 \frac{s}{M} \log q, \quad q \in \mathcal{P}.$$

Indeed, assume that it is false. Define another convex subset of \mathcal{X}_0 :

$$\mathcal{A} = \{(x_q)_{q \in \mathcal{P}, q \leq q_0} : x_q < 2 \frac{s}{M} \log q\}.$$

By our assumption, the convex sets \mathcal{A} and $\text{conv } \mathfrak{B}$ are disjoint; also, \mathcal{A} is an open set. Therefore, we can apply the Hahn-Banach separation theorem, see [19], and conclude the existence of a nonzero sequence $(\mu_q)_{q \in \mathcal{P}}$ such that

$$S = \sup_{(x_q) \in \mathcal{A}} \sum_{q \in \mathcal{P}} \mu_q x_q$$

satisfies

$$\sup_{(x_q) \in \mathcal{A}} \sum_{q \in \mathcal{P}} \mu_q x_q \leq \inf_{(x_q) \in \text{conv } \mathfrak{B}} \sum_{q \in \mathcal{P}} \mu_q x_q.$$

and in particular is finite. Furthermore, since S is finite we also see that $\mu_q \geq 0$ for all q . Hence

$$S = 2 \frac{s}{M} \sum_{q \in \mathcal{P}} \mu_q \log q > 0.$$

Now we define a nonnegative sequence

$$(\lambda_q) = (\mu_q / S)_{q \in \mathcal{P}}.$$

Then we have

$$(5.10) \quad \sum_{q \in \mathcal{P}} \lambda_q \log q \leq \frac{M}{2s}$$

and

$$(5.11) \quad \min_{\mathcal{B} \in \mathfrak{B}} \sum_{q \in \mathcal{B}} \lambda_q \geq 1.$$

We now take

$$\mathcal{Q} = \left\{ q \in \mathcal{P} : |\lambda_q| > \frac{1}{2s} \right\}$$

for which by (5.10) we have (5.8). Thus there exists $\mathcal{B} \in \mathfrak{B}$ with $\mathcal{B} \cap \mathcal{Q} = \emptyset$. We have

$$\sum_{q \in \mathcal{B}} |\lambda_q| \leq \frac{1}{2s} \# \mathcal{B} \leq \frac{1}{2}$$

contradicting (5.11). This proves the existence of $\beta = (\beta_q)_{q \in \mathcal{P}} \in \text{conv } \mathfrak{B}$ satisfying (5.9).

It follows from the condition (ii) and the inequality (5.9) that

$$\sum_{q \in \mathcal{P}} |x_q| \beta_q < 2 \frac{s}{M} \sum_{q \in \mathcal{P}} |x_q| \log q \leq 2 \frac{sL}{M}.$$

Therefore

$$\sum_{\mathbf{x} \in \mathcal{F}} \sum_{q \in \mathcal{P}} |x_q| \beta_q < 2 \frac{sL}{M} \# \mathcal{F}.$$

Since $\beta \in \text{conv } \mathfrak{B}$, by the convexity there is $\mathcal{B} \in \mathfrak{B}$ with

$$\sum_{\mathbf{x} \in \mathcal{F}} \sum_{q \in \mathcal{B}} |x_q| < 2 \frac{sL}{M} \# \mathcal{F}.$$

Hence there is a set $\mathcal{F}_0 \subseteq \mathcal{F}$ such that

$$(5.12) \quad \#\mathcal{F}_0 \geq \frac{1}{2}\#\mathcal{F}$$

and for every $\mathbf{x} \in \mathcal{F}_0$ we have

$$(5.13) \quad \sum_{q \in \mathcal{P}} |x_q| \leq \frac{4SL}{M}.$$

Since $\mathcal{B} \in \mathfrak{B}$, the map $\pi_{\mathcal{B}}$ is one-to-one on \mathcal{F}_0 . Moreover, $x_q \in \mathbb{Z}$ for $\mathbf{x} \in \mathcal{F}$. Therefore, from (5.12) and (5.13) we derive

$$\#\mathcal{F} \leq 2\#\mathcal{F}_0 = 2\pi_{\mathcal{B}}(\mathcal{F}_0) < 2 \binom{\lceil 4sL/M \rceil + s}{s}$$

and the result follows. \square

5.4. Estimating $S_p(K_1, K_2)$.

Lemma 28. *We have*

$$S_p(K_1, K_2) = o(1),$$

as $p \rightarrow \infty$

Proof. By Lemma 23, we have

$$(5.14) \quad \sum_{\substack{k|p-1, \\ K_2 < k \leq K_1}} \frac{T((p-1)/k, p)}{k} \leq \sum_{\substack{k|p-1, \\ K_2 < k \leq K_1}} k^{1/3+o(1)} p^{-1/3} + \sum_{\substack{k|p-1, \\ K_2 < k \leq K_1}} k^{-2/3+o(1)}.$$

The first sum can be estimated trivially:

$$(5.15) \quad \sum_{\substack{k|p-1, \\ K_2 < k \leq K_1}} k^{1/3+o(1)} p^{-1/3} \leq \sum_{K_2 < k \leq K_1} k^{1/3+o(1)} p^{-1/3} \\ \leq K_1^{(4/3)+o(1)} p^{-1/3} = o(1).$$

Next,

$$\begin{aligned} \sum_{\substack{k|p-1, \\ K_2 < k \leq K_1}} k^{-2/3+o(1)} &\ll \sum_{\substack{k|p-1, \\ K_2 < k \leq K_1}} k^{-0.65} \\ &= \sum_{K_2 < k \leq K_1} k^{-0.65} (\tau(p-1, k) - \tau(p-1, k-1)). \end{aligned}$$

By partial summation,

$$(5.16) \quad \sum_{\substack{k|p-1, \\ K_2 < k \leq K_1}} k^{-2/3+o(1)} \ll \sum_{K_2 < k \leq K_1} k^{-1.65} \tau(p-1, k) + K_1^{-0.65} \tau(p-1, K_1).$$

Define q as the largest prime q so that

$$(5.17) \quad \prod_{\substack{\ell \leq q \\ \ell \text{ prime}}} \ell \leq p-1.$$

By (5.7) we have

$$(5.18) \quad q = \log p + o(\log p).$$

Therefore, $q \leq (\log k)^{2.6}$ for $k > K_2$. Using Lemma 26 and Corollary 13 we get

$$\tau(p-1, k) \ll k^{0.62} \quad (k > K_2).$$

Plugging in this estimate to (5.16) we conclude that

$$(5.19) \quad \sum_{\substack{k|p-1, \\ K_2 < k \leq K_1}} k^{-2/3+o(1)} = o(1).$$

Now the result follows from (5.14), (5.15) and (5.19). \square

5.5. Estimating $S_p(K_2, K_3)$.

Lemma 29. *We have*

$$S_p(K_2, K_3) = o(1),$$

as $p \rightarrow \infty$

Proof. For any integer $K \in (K_3, K_2]$ we estimate

$$(5.20) \quad S(K) = \sum_{\substack{k|p-1, \\ K/e < k \leq K}} \frac{T((p-1)/k, p)}{k}.$$

By Corollaries 24 and 26, we have

$$(5.21) \quad S(K) \leq 2\Psi(K, p_s)\Psi(K, q)/K.$$

where $r = r_0(K)$, $s = s_0(K, K)$ and the prime q is defined by (5.17).

To estimate s we use a simple inequality

$$(5.22) \quad \binom{r+s}{s} \geq (r/s)^s.$$

For $K \leq K_2$ we have $r \gg (\log p)^{0.6}$. Take $s_0 = \lfloor (\log p)^{0.4} \rfloor$. Then we have, by (5.22),

$$\binom{r+s_0}{s_0} \geq (\log p)^{0.2+o(1)(\log p)^{0.4}} > K.$$

Consequently, $s \leq s_0 = o(r)$ and

$$(5.23) \quad \binom{r+s}{s} = (r/s)^{s+o(s)} \quad \text{and} \quad \binom{r+s+1}{s+1} = (r/s)^{s+o(s)}$$

Since $r/s_0 \leq r_0/s \leq r$ we have

$$\log(r/s) \asymp \log r \asymp \log((\log p)/\log K),$$

and thus we get the order for s

$$s \asymp \frac{\log K}{\log((\log p)/\log K)}$$

Thus, for $K \leq K_2$ we have

$$\log(r/s) = \log r - \log s = (1 + o(1)) (\log \log p - 2 \log \log K).$$

Hence, from (5.23) and the inequalities

$$\binom{r+s}{s} \leq K < \binom{r+s+1}{s+1}$$

we obtain an asymptotic formula for s :

$$(5.24) \quad s = \frac{\log K}{\log \log p - 2 \log \log K} (1 + o(1)) + O(1) \quad \text{as} \quad K \leq K_2.$$

(Note the term $O(1)$ is included to have a uniform estimate for $2 \leq K \leq K_2$, rather than only in the range $K_3 < K \leq K_2$).

Using that $\log(1 + \alpha) \leq \alpha$ for any $\alpha > 0$, and that $s \rightarrow \infty$ for $K \geq K_3$, we now conclude from Lemma 12 that

$$\log \Psi(K, p_s) \leq (1 + o(1)) \frac{p_s}{\log p_s} \left(1 + \log \left(1 + \frac{\log K}{p_s} \right) \right).$$

Next, by (5.24),

$$\frac{\log K}{p_s} \leq \frac{\log K}{s} \leq (1 + o(1)) \log \log \log p$$

thus, by the prime number theorem,

$$\frac{p_s}{\log p_s} = s + o(s).$$

Using (5.24) again, we deduce

$$(5.25) \quad \begin{aligned} \log \Psi(K, p_s) &\leq (1 + o(1)) \frac{\log K}{\log \log p - 2 \log \log K} \log \log \log p \\ &\leq (1 + o(1)) \frac{5 \log K}{\log \log p} \log \log \log p. \end{aligned}$$

Using Lemma 16 and (5.18) we get

$$\log \Psi(K, q) \leq \log K - (1 + o(1)) \frac{\log K}{\log \log p} \log \frac{\log K}{\log \log p}.$$

Thus, for $K \geq K_3$ we have the inequality

$$(5.26) \quad \log \Psi(K, q) \leq \log K - (1 + o(1)) \frac{6 \log K}{\log \log p} \log \log \log p.$$

Combining (5.25) and (5.26) gives

$$\begin{aligned} \log \Psi(K, p_s) + \log \Psi(K, q) &\leq \log K - (1 + o(1)) \frac{\log K}{\log \log p} \log \log \log p \\ &\leq \log K - (1 + o(1)) \frac{\log K_3}{\log \log p} \log \log \log p \\ &\leq \log K - (1 + o(1)) (\log \log p)^6 \log \log \log p. \end{aligned}$$

Therefore, by (5.21), $S(K) \ll (\log p)^{-2}$. Observing that the sum $S_p(K_2, K_3)$ does not exceed the sum of $O(\log p)$ of sums $S_p(K)$ with $K_3 < K \leq K_2$, we complete the proof. \square

5.6. Estimating $S_p(K_3, 0)$.

Lemma 30. *We have*

$$S_p(K_3, 0) = O(1).$$

Proof. Since $X(k, p) = \emptyset$ for $k^k < p/2$ we can always assume that k is large enough.

For $K \leq K_3$ we estimate the following sums similar to ones given by (5.20):

$$(5.27) \quad S(K) = \sum_{\substack{k|p-1, \\ K/V < k \leq K}} \frac{T((p-1)/k, p)}{k},$$

where

$$(5.28) \quad V = (\log p)^{0.01}.$$

As before, we put $s = s_0(K, K)$.

By (5.24), we have $\log s \leq \log \log K - 1$. Also, $\log r \geq \log \log p - \log \log K - 2$. Therefore,

$$(5.29) \quad \begin{aligned} s &\leq \frac{\log K}{\log \log p - 2 \log \log K} \\ &\leq \tilde{u} \left(1 + O \left(\frac{\log \log \log p}{\log \log p} \right) \right) + O(1), \end{aligned}$$

where

$$(5.30) \quad \tilde{u} = \frac{\log K}{\log \log p}.$$

Identify an integer x given by its prime number factorisation

$$x = \prod_{q \in \mathcal{P}} q^{\sigma_q}$$

with the sequence $(\sigma_q)_{q \in \mathcal{P}}$. Then the set $X(k, p)$ becomes a subset \mathcal{F} of \mathcal{X} of Section 5.3. As can be seen from the proof of Theorem 1 (see (2.1)) it satisfies the condition (i) of Lemma 27. Clearly, it also satisfies the condition (ii) of Lemma 27 with $L = \log K$.

We now fix some M with $1 < M < \log K$ (to be chosen later). Let \mathcal{K}_g be the set of “good” $k \leq K$ for which the condition (iii) of Lemma 27 also holds for $X(k, p)$.

Then the bound of Lemma 27 yields that for $k \in \mathcal{K}_g$ we have

$$(5.31) \quad \#X(k, p) \leq \left(c \frac{\log K}{M} \right)^s$$

for some absolute constant $c > 0$.

Let \mathcal{K}_b be the set of the remaining “bad” $k \leq K$ for which the condition (iii) of Lemma 27 fails.

Now we define a list (a multiset) \mathcal{L} of integers $m \in (K/V, K]$. For any $k \in (K/V, K]$ and for any $l \leq K/k$ we write kl as many as $T((p-1)/k, p)$ times. Thus, we have

$$\#\mathcal{L} = \sum_{\substack{k|p-1, \\ K/V < k \leq K}} T((p-1)/k, p) \left\lfloor \frac{K}{k} \right\rfloor.$$

Hence,

$$(5.32) \quad \sum_{\substack{k|p-1, \\ K/V < k \leq K}} \frac{T((p-1)/k, p)}{k} \leq 2K^{-1} \#\mathcal{L}.$$

For any $m \leq K$ the number of occurrences of m in \mathcal{L} is, by Lemma 22,

$$\sum_{\substack{k|(p-1, m), \\ K/V < k \leq K}} T((p-1)/k, p) \leq \#X((p-1, m), p).$$

We say that m is “good” if $(p-1, m)$ is “good”, and m is “bad” if $(p-1, m)$ is “bad”. We split \mathcal{L} into the sublists \mathcal{L}_g and \mathcal{L}_b formed by “good” and “bad” elements, respectively.

We have

$$\#\mathcal{L}_b = \sum_{\substack{k|p-1, \\ K/V < k \leq K, \\ k \in \mathcal{K}_b}} \#X(k, p) \left\lfloor \frac{K}{k} \right\rfloor.$$

Therefore,

$$(5.33) \quad \#\mathcal{L}_b \leq K \Sigma_b(K),$$

where

$$\Sigma_b(K) = \sum_{\substack{k|p-1, \\ K/V < k \leq K, \\ k \in \mathcal{K}_b}} \frac{\#X(k, p)}{k}.$$

We now estimate $\Sigma_b(K)$.

We assume that $k \in \mathcal{K}_b$. Then for some set $\mathcal{Q} \subseteq \mathcal{P}$ satisfying (5.8) and distinct integers $x_1, x_2 \in X(k, p)$ for the rational number $\gamma = x_1/x_2$ we have

$$(5.34) \quad \gamma = \prod_{q \in \mathcal{Q}} q^{\sigma_q}, \quad \sigma_q \in \mathbb{Z}.$$

Since $x_1, x_2 \in [1, k] \subseteq [1, K]$, we have

$$(5.35) \quad \sum_{q \in \mathcal{Q}} |\sigma_q| \log q \leq 2 \log K.$$

Fix an arbitrary set \mathcal{Q} satisfying (5.8) and estimate the number N of rational numbers γ satisfying (5.34) and (5.35).

For some real parameter $\tau > 0$ we partition \mathcal{Q} as $\mathcal{Q} = \mathcal{Q}_1 \cup \mathcal{Q}_2$ where $\mathcal{Q}_1 = \mathcal{Q} \cap [1, e^\tau]$. A crude estimate gives the bound

$$N \leq N_1 N_2$$

where

$$\begin{aligned} N_1 &= \# \left\{ (\sigma_q)_{q \in \mathcal{Q}_1} : \sum_{q \in \mathcal{Q}_1} |\sigma_q| \leq 2 \log K \right\}; \\ N_2 &= \# \left\{ (\sigma_q)_{q \in \mathcal{Q}_2} : \sum_{q \in \mathcal{Q}_2} |\sigma_q| \leq \frac{2 \log K}{\tau} \right\}. \end{aligned}$$

Since, trivially, $\#\mathcal{Q}_1 \leq e^\tau$ and by (5.8) we also have $\#\mathcal{Q}_2 < M/\tau$, we derive

$$N \leq (4 \log K + 1)^{e^\tau} \left(4 \frac{\log K}{\tau} + 1 \right)^{M/\tau}.$$

Taking $\tau = 0.6 \log M$ we obtain

$$N < (\log K)^{2M/\log M},$$

provided that K is large enough.

Clearly, there are at most e^M possible sets \mathcal{Q} satisfying (5.8). Therefore, we see that there is a finite set $\mathcal{U} \subseteq \mathbb{Q}$ (independent of $k \leq K$) of cardinality

$$\#\mathcal{U} \leq e^M (\log K)^{2M/\log M}$$

such that if $k \in \mathcal{K}_b$ then there are two distinct integers $x_1, x_2 \in X(k, p)$ with $x_1/x_2 \in \mathcal{U}$.

Let r be the multiplicative order of x_1/x_2 modulo p . Since $p \mid x_1^r - x_2^r$ and $1 \leq x_1, x_2 \leq k$ we derive $p \leq k^r$. Hence for $k \leq K \leq K_3$ we have

$$r \geq \frac{\log p}{\log k} > (\log p)^{1/2}.$$

Let \mathcal{R} be the subset of all multiplicative orders modulo p that are greater than $(\log p)^{1/2}$ of all rational number $\gamma \in \mathcal{U}$. Clearly

$$(5.36) \quad \#\mathcal{R} \leq \#\mathcal{U} \leq e^M (\log K)^{2M/\log M}.$$

From the definition of $X(k, p)$ we see that $x_1^k \equiv x_2^k \pmod{p}$. So if r is the multiplicative order of x_1/x_2 then $r \mid k$.

Thus if $k \in \mathcal{K}_b$ then $k \equiv 0 \pmod{r}$ for some $r \in \mathcal{R}$. Thus, the contribution $\Sigma_b(K)$ to $S(K)$ from “bad” k is

$$\Sigma_b(K) = \sum_{\substack{k|p-1, \\ K/V < k \leq K \\ k \in \mathcal{K}_b}} \frac{\#X(k, p)}{k} \leq \sum_{r \in \mathcal{R}} \sum_{\substack{k|p-1, \\ K/V < k \leq K \\ r|k}} \frac{\#X(k, p)}{k}.$$

Applying Corollary 24 and then Corollary 26, we derive

$$\begin{aligned}
 \Sigma_b(K) &\leq \frac{V\Psi(K, p_s)}{K} \sum_{\substack{r \in \mathcal{R} \\ r|p-1}} \tau((p-1)/r, K/r) \\
 (5.37) \quad &\leq \frac{V\Psi(K, p_s)}{K} \sum_{\substack{r \in \mathcal{R} \\ r|p-1}} \Psi(K/r, q)
 \end{aligned}$$

where, as before, the prime q is defined by (5.17).

As we have noticed, only the values of k with $k^k \geq p/2$ are of interest. So we can always assume that

$$K \geq \frac{\log p}{2 \log \log p}.$$

In particular for the parameter \tilde{u} given by (5.30) we have $\tilde{u} \gg 1$.

We also see from (5.29) that

$$\frac{p_s}{\log p_s} \leq \tilde{u} \left(1 + O \left(\frac{1}{\log(\tilde{u} + 1)} \right) \right).$$

So, to estimate $\Psi(K, p_s)$ we use Lemma 12, where we see that the corresponding values of Z satisfies the inequality

$$Z \leq \frac{p_s}{\log p_s} \left(1 + \log \left(1 + \frac{\log K}{p_s} \right) \right).$$

We also note that

$$\frac{\log K}{p_s} \gg \frac{\log K}{\tilde{u} \log(\tilde{u} + 1)} = \frac{\log \log p}{\log(\tilde{u} + 1)} \gg \frac{\log \log p}{\log \log \log p}.$$

Therefore

$$\begin{aligned}
 Z &\leq \frac{p_s}{\log p_s} \left(1 + \log \frac{\log K}{p_s} + o(1) \right) \\
 &= \tilde{u} \left(1 + O \left(\frac{1}{\log(\tilde{u} + 1)} \right) \right) \left(\log \frac{\log K}{\tilde{u} \log(\tilde{u} + 1)} + O(1) \right) \\
 &= \tilde{u} \left(1 + O \left(\frac{1}{\log(\tilde{u} + 1)} \right) \right) \left(\log \frac{\log \log p}{\log(\tilde{u} + 1)} + O(1) \right).
 \end{aligned}$$

We now see from Lemma 12 that

$$\log \Psi(K, p_s) \leq \tilde{u} \left(1 + O \left(\frac{1}{\log(\tilde{u} + 1)} \right) \right) \left(\log \frac{\log \log p}{\log(\tilde{u} + 1)} + O(1) \right).$$

from which we derive

$$(5.38) \quad \log \Psi(K, p_s) \leq \tilde{u} \left(\log \frac{\log \log p}{\log(\tilde{u} + 1)} + O \left(\frac{\log \log \log p}{\log(\tilde{u} + 1)} \right) \right).$$

To estimate $\Psi(K/r, q)$ for $r \geq r_0$ where $r_0 = (\log p)^{1/2}$ we write

$$\Psi(K/r, q) \leq \Psi(K/r_0, q).$$

Then, using (5.18), for

$$u = \frac{\log(K/r_0)}{\log q},$$

we obtain

$$u = \tilde{u} - 1/2 + o(1).$$

Now Lemma 17 yields the estimate

$$(5.39) \quad \Psi(K/r, q) \leq \Psi(K/r_0, q) \ll \frac{K}{r_0} \rho(\tilde{u} - 1/2 + o(1)) \ll \frac{K}{r_0} \tilde{u}^{-\tilde{u}}.$$

Substituting (5.38) and (5.39) in (5.37), we derive

$$\Sigma_b(K) \leq \frac{V \# \mathcal{R}}{r_0} \exp(\xi)$$

where

$$\begin{aligned} \xi &= \tilde{u} \left(\log \frac{\log \log p}{\log(\tilde{u} + 1)} - \log(\tilde{u} + 1) + O \left(\frac{\log \log \log p}{\log(\tilde{u} + 1)} \right) \right) \\ &= \tilde{u} \left(\log \frac{\log \log p}{\tilde{u} \log(\tilde{u} + 1)} + O \left(\frac{\log \log \log p}{\log(\tilde{u} + 1)} \right) \right). \end{aligned}$$

Considering the cases $\tilde{u} \leq (\log \log p)^{1/3}$ and $\tilde{u} > (\log \log p)^{1/3}$ separately, we see that

$$\tilde{u} \frac{\log \log \log p}{\log(\tilde{u} + 1)} = O((\log \log p)^{1/2} + \tilde{u}).$$

Thus

$$(5.40) \quad \Sigma_b(K) \leq V \# \mathcal{R} (\log p)^{-1/2+o(1)} \exp \left(\tilde{u} \left(\log \frac{\log \log p}{\tilde{u} \log(\tilde{u} + 1)} + C \right) \right)$$

for some absolute constant $C > 1$. Considering the cases $\tilde{u} \leq U_1$, $U_1 < \tilde{u} \leq U_2$ and $\tilde{u} > U_2$ separately, where

$$U_1 = \frac{\log \log p}{(\log \log \log p)^2} \quad \text{and} \quad U_2 = e^{2C} \frac{\log \log p}{\log \log \log p},$$

we see that

$$\tilde{u} \left(\log \frac{\log \log p}{\tilde{u} \log(\tilde{u} + 1)} + C \right) \ll \frac{\log \log p \log \log \log \log p}{\log \log \log p} = o(\log \log p).$$

So inserting this bound in (5.40) and recalling (5.28) and (5.36) we arrive to the estimate

$$\Sigma_b(K) \leq e^M (\log K)^{2M/\log M} (\log p)^{-0.49+o(1)}$$

Taking

$$(5.41) \quad M = 10^{-2} \log \log p$$

and recalling (5.33) we finally derive

$$(5.42) \quad \#\mathcal{L}_b \ll K(\log p)^{-1/3}.$$

To estimate $\#\mathcal{L}_g$ we observe that for any “good” m the number of occurrences of m in \mathcal{L} is estimated by the bound (5.31) which with M given by (5.41) becomes

$$\#X((p-1, m), p) \leq (c_0 \tilde{u})^s$$

where $c_0 = 100c$.

The multiset \mathcal{L} contains only elements from the set

$$\mathfrak{L} = \{dl \leq K : d \mid p-1, l \leq V\}.$$

Hence,

$$(5.43) \quad \#\mathcal{L}_g \leq (c_0 \tilde{u})^s \#\mathfrak{L}.$$

We can estimate $\#\mathfrak{L}$ by Lemma 25 as

$$(5.44) \quad \#\mathfrak{L} \leq \Psi(K, q^*),$$

where q^* is the largest prime number with

$$\prod_{\substack{V < \ell \leq q^* \\ \ell \text{ prime}}} \ell \leq p-1.$$

By the prime number theorem,

$$\prod_{\substack{\ell \leq q^* \\ \ell \text{ prime}}} \ell \leq pe^{O(V)}.$$

Using the prime number theorem again and (5.28) we get

$$q^* \leq (1+o(1)) \log(pe^{O(V)}) = (1+o(1)) \log p.$$

By Lemma 17 we have

$$\begin{aligned} \Psi(K, q^*) &\ll K\rho(w) \\ &= K \exp(-w(\log(w+1) + \log \log(w+2) + O(1))), \end{aligned}$$

where

$$w = \tilde{u} = \frac{\log K}{\log q^*} = \tilde{u}(1 + o(1/\log \log p)) = \tilde{u}(1 + o(\tilde{u}^{-1/6})).$$

Therefore,

$$\Psi(K, q*) \ll K\rho(w) = K \exp(-\tilde{u}(\log(\tilde{u}+1) + \log \log(\tilde{u}+2) + O(1))).$$

Combining this inequality with (5.43) and (5.44) we get

$$(5.45) \quad \#\mathcal{L}_g \ll K \exp\left(-\frac{1}{2}\tilde{u} \log \log(\tilde{u}+2)\right).$$

We now see from (5.32), (5.42), and (5.45) that

$$\sum_{\substack{k|p-1, \\ K/V < k \leq K}} \frac{T((p-1)/k, p)}{k} \ll (\log p)^{-1/3} + \exp\left(-\frac{1}{2}\tilde{u} \log \log(\tilde{u}+2)\right).$$

Taking the sum over $K = (\log p)^{\nu/100}$, $100 \leq \nu \leq 100(\log \log p)^6$ with $\tilde{u} = \nu/100$ and for $K = K_3$ with $\tilde{u} = (\log \log p)^6$ we conclude the proof. \square

5.7. Proof of Theorem 11. Theorem 11 follows immediately from the equation (5.5), the asymptotic formula (5.6) and Lemmas 28, 29 and 30.

5.8. Lower bound. To prove (1.14) we recall that for any $d \mid p-1$ we have

$$T(d, p) = \frac{1}{d} \varphi\left(\frac{p-1}{d}\right) + O(p^{1/2+o(1)}),$$

where $\varphi(k)$ is the Euler function, see [16, Proposition 4.3(a)]. Thus for any D , we derive from (5.1) that

$$(5.46) \quad F(p) \geq \sum_{\substack{d|p-1 \\ d \leq D}} dT(d, p) = \sum_{\substack{d|p-1 \\ d \leq D}} \varphi\left(\frac{p-1}{d}\right) + O(Dp^{1/2+o(1)}).$$

Using the trivial bound $\varphi(k) \leq k$ we now obtain

$$(5.47) \quad \sum_{\substack{d|p-1 \\ d \leq D}} \varphi\left(\frac{p-1}{d}\right) = \sum_{d|p-1} \varphi\left(\frac{p-1}{d}\right) + O(p^{1+o(1)}D^{-1}).$$

Also, it is known that

$$(5.48) \quad \sum_{d|p-1} \varphi\left(\frac{p-1}{d}\right) = p-1.$$

Taking $D = p^{1/4}$, we see that (5.46), (5.47) and (5.48) imply (1.14).

5.9. Estimates for almost all primes. Take an arbitrary increasing function $g : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ such that $g(u) \rightarrow \infty$ as $u \rightarrow \infty$. It is easy to see from the proof of Lemma 30 that

$$S(K_3, K_4) = o(1)$$

where

$$K_4 = (\log p)^{g(p)/3}.$$

Combining this with Lemmas 28 and 29, we get

$$\sum_{\substack{k|p-1, \\ k > K_4}} \frac{T((p-1)/k, p)}{k} = 1 + o(1).$$

Therefore, taking

$$\tilde{K}_4 = (\log x)^{g(x)/3}$$

for a sufficiently large x , by the arguments from [1, Section 5] we conclude that the conjecture (1.12) of J. Holden and P. Moree [16] holds for all but at most

$$E(x) \leq \sum_{k \leq \tilde{K}_4} \sum_{j \leq k} \sum_{p|k^k - (-j)^k} 1 \ll \tilde{K}_4^3 = (\log x)^{g(x)}$$

primes $p \leq x$, which substantially improves the bound

$$E(x) \ll \exp \left(12 \frac{\log x}{\log \log x} \right).$$

from [5, Section 5].

ACKNOWLEDGEMENT

The research was carried out while the second author was visiting the Institute for Advanced Study; the hospitality and excellent working conditions of this institution are gratefully appreciated.

The research of S. K. was supported in part by Grant N. 11-01-00329 from the Russian Fund of Basic Researches and that of I. S. by ARC grant DP1092835.

REFERENCES

- [1] E. Bombieri, J. Bourgain and S. V. Konyagin, *Roots of polynomials in subgroups of \mathbb{F}_p^* and applications to congruences*, Int. Math. Res. Notices, **2009** (2009), Art. ID rnn 802, 1–33.
- [2] J. Bourgain, *Mordell's exponential sum estimate revisited*, J. Amer. Math. Soc. **18** (2005), 477–479.
- [3] J. Bourgain, *On the distribution of the residues of small multiplicative subgroups of \mathbb{F}_p* , Israel J. Math. **172** (2009), 61–74.

- [4] J. Bourgain and M. Z. Garaev, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields*, Math. Proc. Cambridge Phil. Soc., **146** (2009), 1–21.
- [5] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, *Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithms*, Int. Math. Res. Notices, **2008** (2008), Art. ID rnn 090, 1–29.
- [6] M. Campbell and C. Pomerance, *Explicit estimates on some problems concerning primitive roots*, Preprint, 2002.
- [7] T. H. Chan and I. E. Shparlinski, *On the concentration of points on modular hyperbolas and exponential curves*, Acta Arith., **142** (2010), 59–66.
- [8] J. Cilleruelo and M. Z. Garaev, *Concentration of points on two and three dimensional modular hyperbolas and applications*, Preprint, 2010 (available from <http://arxiv.org/abs/1007.1526>).
- [9] J. Cilleruelo and J. Jiménez Urroz, *The hyperbola $xy = N$* , J. Théorie des Nombres de Bordeaux, **12** (2000), 87–92.
- [10] C. Cobeli and A. Zaharescu, *An exponential congruence with solutions in primitive roots*, Rev. Roumaine Math. Pures Appl., **44** (1999), 15–22.
- [11] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997.
- [12] D. Grigoriev and G. Tenenbaum, *A low complexity probabilistic test for integer multiplication*, J. Complexity, **26** (2010), 263–267.
- [13] A. Hildebrand and G. Tenenbaum, *Integers without large prime factors*, J. Théorie des Nombres de Bordeaux, **5** (1993), no. 2, 411–484.
- [14] J. Holden, *Fixed points and two cycles of the discrete logarithm*, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, **2369** (2002), 405–416.
- [15] J. Holden and P. Moree, *New conjectures and results for small cycles of the discrete logarithm*, High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, Fields Institute Communications, **41** (2004), Amer. Math. Soc., 245–254.
- [16] J. Holden, P. Moree, *Some heuristics and results for small cycles of the discrete logarithm*, Math. Comp. **75** (2006), 419–449.
- [17] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999.
- [18] J. F. Koksma, *Some theorems on diophantine inequalities*, Math. Centrum Scriptum no. 5, Amsterdam, 1950.
- [19] W. Rudin, *Functional analysis*, McGraw-Hill Science/Engineering/Math, 1991.
- [20] P. Szűsz, *On a problem in the theory of uniform distribution*, Comptes Rendus Premier Congrès Hongrois, Budapest, 1952, 461–472 (in Hungarian).
- [21] W. P. Zhang, *On a problem of Brizolis*, Pure Appl. Math., **11** (1995), suppl., 1–3 (in Chinese).

SCHOOL OF MATHEMATICS, INSTITUTE FOR ADVANCED STUDY, PRINCETON,
NJ 08540, USA

E-mail address: bourgain@math.ias.edu

STEKLOV MATHEMATICAL INSTITUTE, 8, GUBKIN STREET, MOSCOW, 119991,
RUSSIA

E-mail address: konyagin@mi.ras.ru

DEPARTMENT OF COMPUTING, MACQUARIE UNIVERSITY, NORTH RYDE, SYD-
NEY, NSW 2109, AUSTRALIA

E-mail address: igor.shparlinski@mq.edu.au